VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zabezpečení datové komunikace pomocí bezpečnostní brány firewall ASA
Security of Data Communication by ASA Firewall

2012 **Jaroslav Laš**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Jaroslav Laš**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Zabezpečení datové komunikace pomocí bezpečnostní brány firewall ASA
Security of Data Communication by ASA Firewall

Zásady pro vypracování:

Bezpečnostní brány poskytují řadu funkcí pro zajištění bezpečnosti uvnitř sítě. Cílem bakalářské práce je navrhnout možné řešení s prvky ASA a toto řešení ověřit v laboratoři.
1. Seznámení s problematikou firewallů.
2. Konfigurace a správa bezpečnostní brány.
3. Ověření funkčnosti v laboratoři pomocí nástroje hping2.

Seznam doporučené odborné literatury:

Frahim J., Santos O. *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance.* Cisco Press 2010
Dále podle pokynů vedoucího bakalářské práce.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Pavel Nevlud**

Datum zadání: 18.11.2011
Datum odevzdání: 04.05.2012

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * OSTRAVA

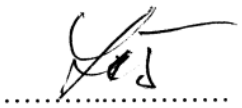
prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prehlásenie študenta

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

Dňa: 2.5. 2012



Poďakovanie

Rád by som poďakoval Ing. Pavlovi Nevludovi za odbornú pomoc a konzultácie pri vytváraní tejto bakalárskej práce.

Abstrakt

Téma bezpečnosť počítačovej siete je v dnešnej dobe na popredných miestach riešených problémov. Okrem samotnej ochrany dát a odopretiu prístupu neautorizovaným osobám, bezpečnosť obsahuje aj detekciu nežiaducej udalosti, prevenciu, ktorá sa vykonáva podľa daných krokov pri detekcii útoku. Cieľom tejto bakalárskej práce bolo popísať základnú problematiku práce a funkčnosti bezpečnostnej brány, použitie rôznych filtračných techník a navrhnúť možné riešenie za pomoci prvku Cisco ASA 5505. Pre tieto navrhnuté riešenia vytvoriť konfigurácie a následne ich otestovať a overiť ich funkčnosť v laboratóriu pomocou sieťových nástrojov: Hping2, Wireshark, Packet Tracer.

Kľúčové slová

Bezpečnostná brána, filtrácia, konfigurácia, testovanie, prevencia, Cisco ASA, Hping

Abstract

The safety of computer network takes nowadays the leading places of solving issues. In addition the data protecting and refusing to access to unauthorized persons, the security also includes undesirable event detection, prevention, which is performed by following steps in the detection of the attack. The purpose of this bachelor thesis is to describe the basic issues of job security and functionality of the gateway, using different filtering techniques and propose a possible solution using Cisco ASA 5505. For these proposed solutions the configuration was created and then tested. For verification of the functionality in the laboratory was used network tools Hping2, Wireshark and Packet Tracer.

Key words

Gateway, filtering, configuration, testing, prevention, Cisco ASA, Hping

Zoznam použitých skratiek

Skratka	Anglický význam	Slovenský význam
NAT	Network Address Translation	Preklad sieťovej adresy
OSI	Open Systems Interconnection	Referenčný model
FTP	File Transfer Protocol	
HTTP	Hypertext Transfer Protocol	
TCP	Transmission Control Protocol	
IP	Internet Protocol	
UDP	User Datagram Protocol	
ACL	Access Control List	
PAT	Port Address Translation	
VPN	Virtual Private Network	
IPS	Intrusion Prevention System	
IDS	Intrusion Detection System	
DoS	Denial of Service	Odmietnutie služby
DDoS	Distributed Denial of Service	Distribuované DoS
IPsec	IP Security	
HTTPS	Hypertext Transfer Protocol Secure	
ICMP	Internet Control Message Protocol	
SSH	Secure Shell	
WWW	World Wide Web	
ASDM	Adaptive Security Device Manager	
VLAN	Virtual Local Area Network	Virtuálna lokálna sieť
DMZ	Demilitarized Zone	Demilitarizovaná zóna
XSS	Cross-site scripting	
SQL	Structured Query Language	Štruktúrovaný dotazovací jazyk

Obsah

1 Úvod

Firewall je špeciálny počítač, ktorý je jediným spojovacím článkom medzi vonkajšou sieťou (Internet) a vnútornou sieťou. Tento počítač neposkytuje vonkajšiemu svetu informácie o smerovaní vo vnútornej sieti a spôsobuje tak, že vnútorná sieť je pred vonkajším svetom neviditeľná.

Slúži k riadeniu a zabezpečeniu sieťovej premávky medzi sieťami s rôznou úrovňou zabezpečenia a dôveryhodnosti. Dá sa povedať, že slúži ako kontrolný bod, ktorý definuje pravidlá komunikácie medzi sieťami. Tieto pravidlá zahrňovali identifikáciu zdroja cieľa dát, ale pre dnešné bezpečnostné brány pomerne nedostatočné. Moderné bezpečnostné brány sa opierajú o informácie o stave spojenia, znalosť kontrolovaných protokolov a prípadne prvky IDS.

Firewall je možné považovať za inteligentné zariadenie, ktoré sleduje obsah prichádzajúcich paketov a rozhoduje, čo sa bude s paketom diať. Paket môže byť doručený na cieľovú adresu, zahodený alebo firewall môže prepísať hlavičku napríklad za účelom prekladu adresy. Môže tiež riešiť autentizáciu užívateľov vstupujúcich do vnútornej siete.

Počítače sa stali súčasťou takmer každej profesie. Internet sa rozšíril do mnohých domácností a je nutnosťou takmer pre každú firmu. Nejedna firma má viacero pobočiek, ktoré si navzájom vymieňajú informácie, rôzne dáta a komunikujú medzi sebou. So stúpajúcim počtom užívateľov stúpol aj počet útokov na vnútorné siete a poskytované služby. Medzi prvotné problémy sa tak stáva otázka bezpečnosti.

Cieľom tejto bakalárskej práce je zoznámiť sa so základnou problematikou práce a funkčnosťou bezpečnostnej brány, navrhnúť možné riešenie za pomoci prvku Cisco ASA 5505. Následne predviesť konfiguráciu jednotlivých návrhov a správu bezpečnostnej brány. Vytvorené riešenia následne otestovať a overiť ich funkčnosť v laboratóriu pomocou nástroja hping2 alebo podobným nástrojom.

Prvá časť tejto bakalárskej práce (kapitola 2) je zameraná na zoznámenie sa s problematikou firewallov, jej popis a používané bezpečnostné techniky (podkapitoly 2.1, 2.2 a 2.3). Ďalej je v tejto časti uvedený popis a využitie prístupových zoznamov, pomocou ktorých môžeme povoľovať alebo obmedzovať sieťovú premávku celej siete alebo jednotlivých užívateľov k jednotlivým službám alebo k Internetu (podkapitola 2.4). Dôležitou časťou je popis princípu prekladu vnútorných adries na verejné adresy (podkapitola 2.5) a možnosti techník a zabezpečenia prepojení privátnych sietí pomocou VPN (podkapitola 2.6). Ďalej sú popísané systémy, ktorých hlavnou úlohou sú monitorovanie a odhaľovanie škodlivých aktivít alebo útokov (podkapitoly 2.7 a 2.8). Na konci tejto sekcie sú uvedené základné sieťové útoky (podkapitola 2.9).

Druhá časť (kapitola 3) je zameraná na návrh a implementáciu. V úvode kapitoly je stručný popis bezpečnostnej brány (podkapitola 3.1) a možnosti pripojenia a komunikácie (podkapitola 3.2). Ďalej sa nachádza jednoduché schéma, jej konfigurácia a popis jednotlivých parametrov (podkapitola 3.3), popis a využitie možností riadeného NAT (podkapitola 3.4). Nasleduje ďalšie riešenie, v ktorom sú povoľované jednotlivé služby pre prístup do vonkajšej siete (podkapitola 3.5) a z týchto služieb vytvorené skupiny objektov (podkapitola 3.6) pre zjednodušenie správy bezpečnostnej brány. V závere kapitoly sa nachádza stručný popis webového prostredia ASDM (podkapitola 3.7) a overenie komunikácie sieťovými nástrojmi na základe použitej konfigurácie (podkapitola 3.8).

Záver tejto práce je venovaný celkovému vyhodnoteniu dosiahnutých výsledkov.

2 Firewall

Firewall je sieťové zariadenie alebo softvér, ktorého úlohou je oddeliť siete s rôznymi prístupovými právami (typicky napr. Internet a vnútorná sieť) a kontrolovať tok dát medzi týmito sieťami.

Kontrola údajov prebieha na základe aplikovania pravidiel, ktoré určujú podmienky a akcie. Podmienky sa stanovujú pre údaje, ktoré možno získať z dátového toku (napr. zdrojová, cieľová adresu, zdrojový alebo cieľový port, a rôzne iné). Úlohou firewallu je vyhodnotiť podmienky a ak je podmienka splnená, vykoná sa akcia. Dve základné akcie sú "povoliť dátový tok" a "zamietnuť dátový tok". Po vykonaní takejto akcie firewall prestane paket spracovávať. Existujú však aj iné akcie, ktoré neurčujú osud paketu a slúžia napr. na logovanie hlavičiek paketu, zmenu hlavičiek paketu a podobne.

Ďalšou vlastnosťou firewallu, ktorá sa často používa, je schopnosť prekladu adries NAT (Network Address Translation). NAT umožňuje zmeniť zdrojové a cieľové adresy v paketoch, čím sa najčastejšie umožňuje komunikácia so sieťami s privátnymi adresami.

Podľa toho, na ktorej vrstve firewall analyzuje sieťovú prevádzku, rozlišujeme v zásade dva firewally:

- Proxy server
- Paketový filter

2.1 Osobný firewall

Osobné firewally používajú podobné metódy ako sieťové firewally. Poskytujú filtračné techniky a stavovú kontrolu riadeného spojenia k špecifickému hostiteľovi. Tieto aplikácie môžu obmedzovať prístup k službám a aplikáciám inštalovaných jedným hostiteľom. To sa často umiestňuje pobočkám a vzdialeným mobilným užívateľom.

2.2 Proxy server

Proxy [1] sa prevažne používa na rozhraní dvoch sietí, medzi ktorými nie je priama konektivita. Používa sa ako oddeľovač obidvoch sietí. Z jednej siete je možné sa pripojiť k proxy

a z nej potom do druhej siete. Klasická predstava je počítač s dvomi sieťami a sieťovými rozhraniami do každej z nich.

Pracuje tak, že serverová časť proxy posiela požiadavky klientskej časti proxy a opačne. Pri posielaní požiadaviek medzi týmito dvomi časťami proxy nemusí dôjsť len k mechanickému posielaniu.

Jedná sa o filtrovanie na aplikačnej vrstve referenčného modelu OSI, t.j. aplikačný proxy server dokáže presne analyzovať celú sieťovú prevádzku a význam paketov na najvyššej vrstve. Tak môže chrániť napr. pred vírusmi alebo rôznym škodlivým obsahom a umožňovať prístup na základe autentifikácie používateľa.

Nevýhodou aplikačného proxy servera je spomalenie sieťovej prevádzky, pretože kvôli analýze údajov musí skladať všetky pakety až po aplikačnú vrstvu. Ďalšou nevýhodou je, že aplikačné proxy servery nie sú univerzálne a väčšinou treba používať špecifický proxy server pre každý typ komunikácie. Typické príklady sú napr. HTTP proxy servery, FTP proxy servery a iné.

2.3 Paketový filter

Paketový filter umožňuje kontrolovať prechádzajúce pakety aktívnym prvkom siete na základe jeho obsahu. Filtrácia sa môže vykonávať na rôznych úrovniach:

- Na linkovej vrstve
- Filtrácia protokolov TCP a IP
- Filtrácia aplikačných protokolov

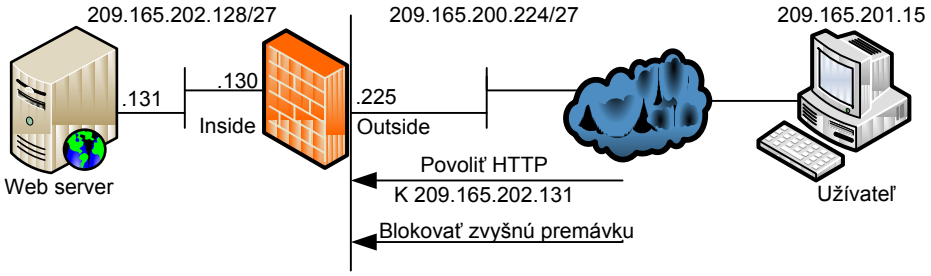
Pri filtrácii na linkovej vrstve, musí filter poznať linkové záhlavie, pretože sa filtruje na základe informácii uvedených v linkovom záhlaví každého rámca.

V prípade filtrácie na úrovni protokolu IP musí filter poznať záhlavie IP datagramu, teda na základe IP adresy odosielateľa a príjemcu. V prípade filtrácie na úrovni protokolu TCP zase filter musí poznať záhlavie TCP segmentu. Kombináciu protokolu IP a protokolov TCP/UDP je možné stanoviť, aby konkrétne počítače mohli medzi sebou komunikovať len konkrétnymi aplikáciami.

Iná situácia je pri filtrácii aplikačných protokolov, ktoré často neobsahujú záhlavie. V takom prípade musí filter rozumieť celému aplikačnému protokolu a filtrovať všetky aplikačné dáta.

Pri tvorbe filtru sú teoreticky možné dve varianty. Buď sa všetko povolí a dopisujú sa pravidlá špecifikujúce, ktoré počítače kam nemôžu. Alebo naopak sa všetko zakáže a postupne sa niečo povoľuje. Z bezpečnostných dôvodov sa väčšinou dáva prednosť druhej variante.

Nevýhodou paketového filtra je aj to, že niekedy musia na serveri fungovať služby, ktoré pri komunikácii využívajú náhodne vybrané porty (napr. pri prenose súborov pomocou FTP). Paketový filter nevidí súvislosti medzi paketmi a každý analyzuje samostatne. Vtedy treba buď povoliť celý rozsah portov, alebo ho zakázať a takéto služby nepoužívať.



Obrázok 2.1 Príklad filtrovania paketov.

2.4 Stavový firewall

Stavový firewall si na rozdiel od paketového filtra navyše udržuje tabuľku všetkých nadviazaných spojení, ktoré mu slúžia pre zisťovanie, či pakety patria k niektorému otvorenému spojeniu alebo nie. Vytvorené spojenia sú vymazané z tabuľky po vyčerpaní časového limitu.

2.5 Prístupový zoznam

Prístupový zoznam ACL (access list) [2] je v praxi zoznam podmienok, ktoré charakterizujú pakety a môžu byť užitočné pri získaní kontroly nad sieťovou prevádzkou. Môžeme ich napríklad nastaviť tak, aby prijímali konkrétne rozhodnutia, takže k webovým prostriedkom v Internete získajú prístup len určitý užívatelia, ale iní budú mať prístup obmedzený. Pri porovnávaní paketov podľa prístupového zoznamu platí niekoľko dôležitých pravidiel:

- Paket sa vždy porovnáva s každým riadkom v zozname v pevnom poradí. To znamená, že sa vždy začína od prvého riadku v zozname a postupne prechádza ďalšie riadky
- Porovnávanie s riadkami v zozname prebieha tak dlho, kým sa nenájde zhoda. Keď je paket zhodný s podmienkou v zozname, spracuje sa a ukončí sa ďalšie porovnávanie.
- Na konci každého zoznamu sa nachádza príkaz „deny“. Ak teda paket nevyhovuje podmienke zo žiadneho riadku v zozname, je zahodený.

Prístupové zoznamy sa delia na dva hlavné typy:

- *Štandardné* – tieto zoznamy používajú ako testovaciu podmienku len zdrojovú IP adresu v pakete IP. Všetky rozhodnutia sa založené na zdrojovej IP adrese. To znamená, že štandardné prístupové zoznamy v zásade povoľujú alebo zakazujú celé sady protokolov (napr. HTTP, Telnet, UDP).
- *Rozšírené* – umožňujú vyhodnocovať mnohé ďalšie polia 3. a 4. vrstvy IP paketu. Môžu analyzovať zdrojovú a cieľovú IP adresu, pole protokolu v hlavičke sieťovej vrstvy a číslo portu v hlavičke transportnej vrstvy.

Vytvorený prístupový zoznam sa neprejaví, pokiaľ ho neaplikujeme. Nie sú aktívne, pokiaľ ich neaplikujeme na rozhranie aktívneho prvku a navyše musíme určiť smer prevádzky. Môžeme požadovať odlišné pravidlá pre odchádzajúcu prevádzku z vnútornej siete do Internetu, ako pre prichádzajúcu prevádzku z Internetu do vnútornej siete.

- *Prichádzajúce prístupové zoznamy* – keď sa pravidlá aplikujú na prichádzajúce rozhranie, sú tieto pakety spracované skôr ako sú odoslané na odchádzajúce rozhranie.
- *Odchádzajúce prístupové zoznamy* – ak sú pravidlá aplikované na odchádzajúce rozhranie, pakety sú odoslané na rozhranie a tam sú spracovávané skôr ako sú zaradené do fronty

2.5.1 Štandardný prístupový zoznam

Filtrovanie sieťovej prevádzky je na základe zdrojovej IP adresy v pakete. Tieto zoznamy je možné vytvárať pod číslami access-list od 1 do 99 alebo od 1 300 do 1 999. Pomocou čísiel z tohto rozsahu bude aktívny prvok očakávať syntax, ktorá definuje len zdrojovú IP adresu.

Príklad štandardného ACL:

```
ciscoasa(config)# access-list dest_net standard permit host
192.168.10.100
```

2.5.2 Rozšírený prístupový zoznam

Tieto zoznamy dovoľujú určiť zdrojovú a cieľovú adresu, protokol a číslo portu, ktoré identifikujú protokol alebo aplikáciu vyššej vrstvy. Pomocou týchto zoznamov môžeme účinne povoliť užívateľom prístup do fyzickej siete LAN a zakázať im prístup ku konkrétnym hostiteľom

alebo určitým službám týchto hostiteľov. Rozšírený zoznam môžeme číslovať v rozsahu od 100 do 199 a je k dispozícii aj rozsah od 2 000 do 2 699.

Príklad rozšíreného ACL:

```
ciscoasa (config) # access-list 100 extended permit icmp any host
158.196.1.2 echo
```

2.6 Network Address Translation

Preklad adries NAT vznikol hlavne preto, aby sa spomalilo vyčerpávanie dostupného adresného priestoru IP. Umožňuje reprezentovať viacero privátnych IP adries menším počtom verejných IP adries. Aplikačné proxy prekladajú vnútorné užívateľské IP adresy na verejnú smerovaciu adresu. NAT prekladá adresy z lokálnej siete na jedinečnú adresu, ktorá slúži pre vstup do inej siete (napr. Internetu). Preloženú adresu si uloží do tabuľky pod náhodným portom, pri odpovedi si v tabuľke vyhľadá port a pošle pakety na IP adresu priradenú k danému portu. NAT je častejšie používaný na firewaloch.

Rozsah adries	*Sieť/maska*
10.0.0.0–10.255.255.255	*10.0.0.0/8*
172.16.0.0–172.31.255.255	*172.16.0.0/12*
192.168.0.0–192.168.255.255	*192.168.0.0/16*

Tabuľka 2.1: Rozsah privátnych adries

Výhody	*Nevýhody*
Šetrí komerčne registrované adresy.	*Preklad spôsobuje oneskorenie.*
Obmedzuje výskyt prekrývajúcich sa adries.	*Stráca sa možnosť sledovať IP adresy medzi koncovými zariadeniami.*
Zvyšuje pružnosť pripojenia k Internetu.	*Niektoré aplikácie pri povolenom NAT nefungujú.*
Eliminuje prečíslovanie adries pri zmene siete.	

Tabuľka 2.2: Výhody a nevýhody implementácie NAT

2.6.1 Statický NAT

Tento typ prekladu adries NAT umožňuje mapovanie lokálnych a globálnych adries podľa schémy 1:1. Táto verzia vyžaduje, aby mal každý užívateľ v sieti reálnu IP adresu v Internete. Prevodná tabuľka „tabuľka NAT“ obsahuje vždy IP adresu vnútornej siete a IP adresu, pod ktorou má adresa vnútornej siete vystupovať v Internete[3].

IP adresa vnútornej siete	*Verejná IP adresa v Internete*
10.1.2.27	*209.165.201.10*
10.1.2.28	*209.165.201.11*
10.1.2.30	*209.165.201.14*

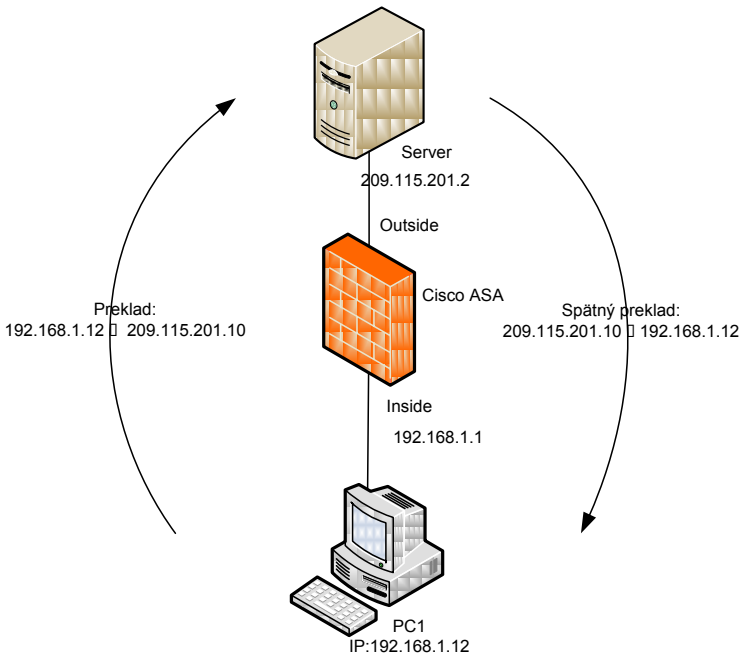
Tabuľka 2.3: Príklad tabuľky NAT

2.6.2 **Dynamický NAT**

Táto verzia umožňuje mapovať vnútornú IP adresu na verejnú IP adresu z príslušného rozsahu. Oproti statickému NAT-u nie je nutné konfigurovať každú adresu, aby mapoval vnútornú adresu na verejnú. Potrebné je mať k dispozícii dostatok reálnych adries pre každého užívateľa, ktorý bude odosielať pakety do Internetu alebo ich prijímať. V prvku NAT existuje NAT Pool. NAT Pool je zoznam verejných adries na odchádzajúcom (outside) rozhraní [4]. Je to v podstate množina adries, ktoré máme k dispozícii pre prístup do vonkajšej siete.

Ako funguje dynamický NAT:

- Počítač z vnútornej siete sa pokúsi spojiť s počítačom alebo serverom z vonkajšej siete.
- NAT prvok prijme paket.
- Ak nemá vnútorná adresa pridelenú adresu, na ktorú sa má prekladať, NAT prvok pridelí prvú dostupnú adresu z NAT Poolu a vytvorí záznam do NAT tabuľky.
- V IP hlavičke paketu sa zmení adresa z vnútornej na verejnú a pošle paket na cieľovú adresu.
- Keď príde požiadavka späť, skontroluje sa cieľová adresa, porovná ju s adresou v NAT tabuľka a zistí, ktorému zariadeniu patrí. Následne sa v IP hlavičke zmení verejná adresa na vnútornú.



Obr. 2.2Príklad prekladu NAT.

Príklad konfigurácie NAT:

```
ciscoasa(config)# nat (inside) 1 10.1.2.0 255.255.255.0
ciscoasa(config)# global (outside) 1 209.165.201.1-209.165.201.15
```

2.6.3 **Preťažený NAT**

Preťaženie je forma dynamického NAT, ktorý mapuje viacero vnútorných adries na jedinú verejnú adresu (1:N) s použitím viacero portov. Tento mechanizmus sa označuje ako PAT (NAT overloading) [5]. S použitím PATu môžeme k Internetu pripojiť až niekoľko tisíc užívateľov pomocou jedinej verejnej IP adresy, teoreticky až 65 000.

Ako funguje PAT:

- Počítač z vnútornej siete sa pokúsi spojiť s počítačom alebo serverom z vonkajšej siete.
- NAT prvok prijme paket.
- Ak tento paket nemá žiadny záznam v NAT tabuľke, vytvorí sa nový záznam a uloží sa do tabuľky s vnútornou adresou a vnútorným prideleným portom. NAT ďalej

pridelí nepoužitý verejný port a svoju verejnú adresu, na ktorú sú mapované všetky pakety z vnútornej siete.

- V IP hlavičke sa vymení adresa a port podľa NAT tabuľky.
- Keď príde požiadavka späť, skontroluje sa cieľová adresa a port, porovná ju v NAT tabuľka a zistí, ktorému zariadeniu patrí. Následne sa v IP hlavičke zmení verejná adresa a port na vnútorné.

Protokol	*IP adresa a port vnútornej siete*	*IP adresa a port v Internete*
TCP	*10.1.2.27:1024*	*209.165.201.10:1024*
TCP	*10.1.2.28:1024*	*209.165.201.11:1025*
UDP	*10.1.2.30:1025*	*209.165.201.14:1028*
TCP	*10.1.2.32:1024*	*209.165.201.15:1029*

Tabuľka 2.4: Príklad NAT tabuľky s použitím PAT

2.7 Virtual Private Network

VPN (Virtual Private Network) [6] je počítačová sieť, ktorej niektoré spojenia medzi uzlami vedú po inej sieti ako je privátna. Jedná sa o takzvané tunelovanie. Dáta prúdiace vo VPN sú typicky zašifrované, ale nie je to podmienkou. Myšlienkou bolo vytvoriť spojenie, v ktorom by boli prenášané dáta, medzi dvoma bodmi naprieč verejnou sieťou.

Vo všeobecnosti je používaná sieť Internetu na prepojenie privátnych sietí alebo prístup k nim. Dáta sú šifrované a oba konce VPN site sa autentifikujú. Výhodou je, že informácie sú tak chránené proti zneužitiu. Ďalšia výhoda je, že ak sa niektorý používateľ pripojí do privátnej siete VPN, jeho stanica vystupuje, akoby bola v privátnej sieti a tým môže využívať všetky dostupné služby v privátnej sieti.

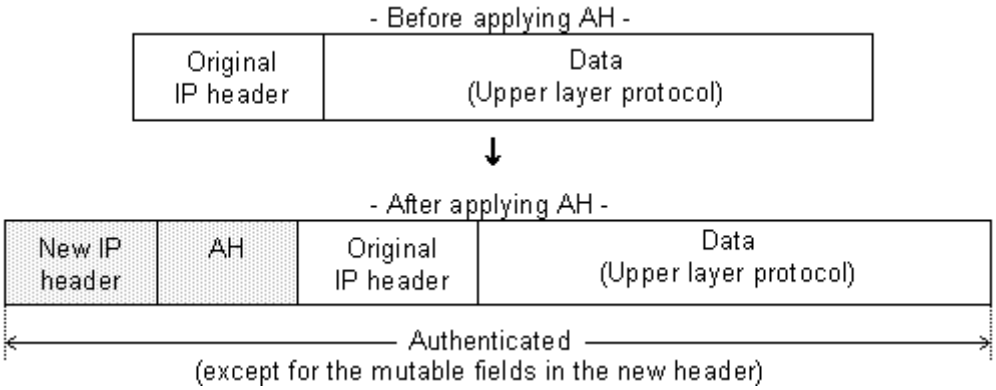
- *Site-to-Site VPN* – spojuje dve alebo viac sietí dohromady, väčšinou centrálu a pobočky. Používajú sa špeciálne sieťové zariadenia (VPN koncentrátory, firewall, router, server), ktoré slúžia ako VPN brány a vytvoria medzi sebou VPN spojenie. Užívateľské stanice potom nepotrebujú VPN klienta.
- *Remote Access VPN* – pripájanie individuálnych užívateľov do lokálnej siete, do ktorej musí mať každý užívateľ špeciálny softvér - VPN klient.

2.7.1 IPsec

IPsec (Internet Protokol Security) je štandardizovaná skupina protokolov pre zabezpečenie IP komunikácie medzi dvomi koncovými systémami. Obsahuje obojsmernú autentifikáciu a vyjednávanie kryptografických metód a kľúčov.

IPsec najskôr zaistí, aby sa obidve strany navzájom identifikovali a potom sa celá komunikácia šifruje pomocou dohodnutého algoritmu.

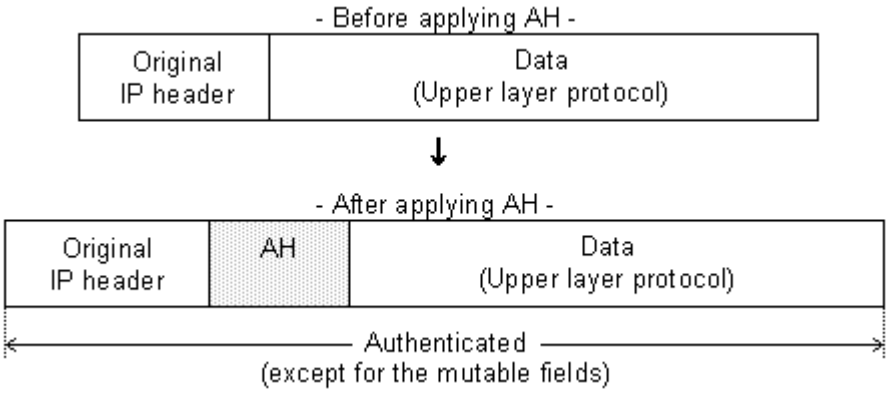
- *Tunelový mód* – šifruje celý paket, vrátane hlavičky, a doplňuje novú hlavičku. Tento mód sa môže použiť pre IPsec proxy, klient posiela dáta, smerovač ich šifruje a posiela ďalej. Z takejto komunikácie sa nedá odhaliť adresa klienta.



Obrázok 2.3 Rozšírenie hlavičky v tunelovom móde.

AH – Autentication header

- *Transparentný mód* – šifruje len dáta, IP hlavička je nezmenená a doplní sa len IPsec hlavička.



Obrázok 2.4 Rozšírenie hlavičky v transparentnom móde.

2.8 Intrusion Detection System

Intrusion detection system (IDS) [7] deteguje nechcenú manipuláciu s počítačovými systémami, ktoré sa v najväčšej miere vykonáva prostredníctvom internetu. Je to technika odhaľovania neoprávnenej alebo nesprávnej aktivity siete. Ide o súbor opatrení, ktoré zabezpečia, že v prípade neoprávneného prieniku do siete bude toto správanie identifikované.

Hlavné spôsoby monitorovania útokov sú založené na detekcii známej sekvencii znakov v komunikácii a analýze protokolov. Typicky ide o program, ktorý sa stará o identifikáciu prienikov.

Podľa spôsobu prístupu ochrany rozlišujeme IDS:

- Uzlovo orientované IDS – Host-Based IDS (HIDS).
- Sieťovo orientované IDS – Network-Based IDS (NIDS).

Uzlovo orientované IDS sú inštalované na lokálnych zariadeniach, čo ich robí veľmi všestrannými v porovnaní so sieťovo orientovanými. Môžu sa inštalovať na mnohých typoch serverov, pracovných staniciach alebo notebookoch. Sú efektívne v detegovaní vnútorných pokusoch o útok.

Sieťovo orientované sa najčastejšie používajú v sieťach, ktoré využívajú prepínače. Ak chceme filtrovať celú premávku, potrebujeme umiestniť snímače na miesta, kde je možné odchytiť čo najväčšiu komunikáciu. NIDS sú najlepšie v detegovaní vonkajších neautorizovaných prístupov a útokov typu DoS.

2.9 Intrusion Prevention System

Intrusion prevention system (IPS) [8] je zariadenie, ktoré monitoruje sieť a zisťuje či sa v nej nenachádzajú nechcené aktivity a prípadne reaguje podľa nastavení administrátora. Keď je útok odhalený, môže tento systém na základe pravidiel zakázať jednotlivé pakety, pričom zvyšná premávka ostáva nezmenená.

Existujú dva typy riešení IPS:

- *In-line IPS* – je umiestnené medzi verejnou a privátnou sieťou, ktorú chceme chrániť. Všetka premávka paketov musí prechádzať IPS, ktoré robí jej analýzu a môže zakázať daný tok.
- *Out-of-band IPS* – umožňuje sledovať premávku prechádzajúcu zo a do privátnej siete bez toho, aby bol fyzicky medzi nimi. Napodobní prerušenie spojenia, ktoré zapríčiní, že cieľový počítač nespracuje škodlivé dáta.

2.10 Sieťové útoky

Cieľom útokov na počítače alebo servery je získať prístup k terminálom cez nejaký nechránený port a získavať potrebné informácie. Útok na počítačovú sieť je zameraný na dátovú komunikáciu alebo na konkrétne služby vo vnútri siete.

Poznáme niekoľko druhov útokov na sieť:

- DoS útok
- DDoS útok
- Session hijacking
- Sniffing
- Neautorizovaný útok
- Aplikačné útoky (XSS, SQL injection)

2.10.1 Denial of Service

Denial of Service (DoS) [9] alebo odmietnutie služby sa využíva k narušeniu služby jedného systému alebo celej siete. Útočník využíva tento typ útoku k preťaženiu alebo vyradeniu systému alebo sieťových zdrojov. Tieto útoky môžu sieťovým zariadeniam blokovať pakety, jednotlivé

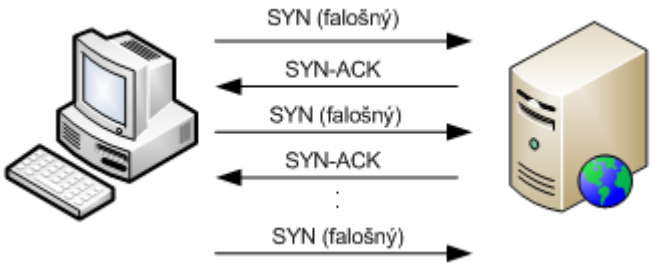
aplikácie môžu prestať správne fungovať. Útočník sa snaží zabrániť systému alebo užívateľom siete používať konkrétnu aplikáciu.

Najčastejšie sa DoS útoky snažia poškodiť pripojenie k sieti, pri pokuse o vytvorenie spojenia sa falšujú TCP a UDP spojenia. Cieľové zariadenie sa snaží zvládnuť ďalšie spojenie a spotrebuje všetky svoje dostupné zdroje.

Typy DoS útokov:

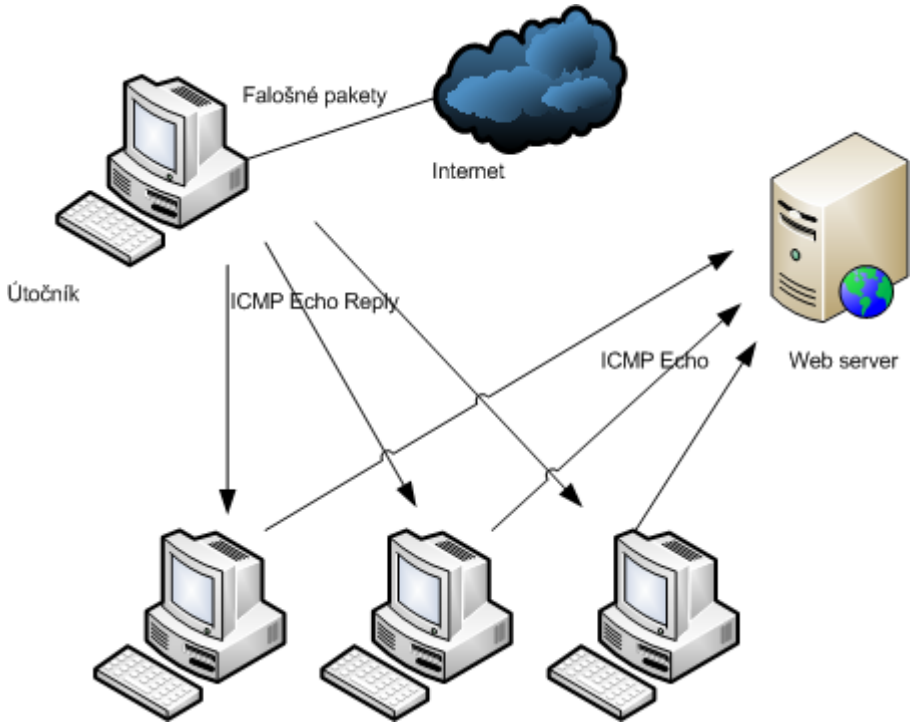
- Záplava TCP SYN
- Smurf

Záplava paketmi SYN alebo tiež SYN-flood posiela množstvo SYN (synchronize) požiadaviek na cieľový server. Server odošle odpoveď ACK (acknowledge), ale útočník neodpovedá konečným ACK k úspešnému ukončeniu spojenia. To zamestnáva server, až kým mu nedôjdu systémové prostriedky a nemôže odpovedať bežným požiadavkám.



Obr. 2.5: Záplava TCP SYN

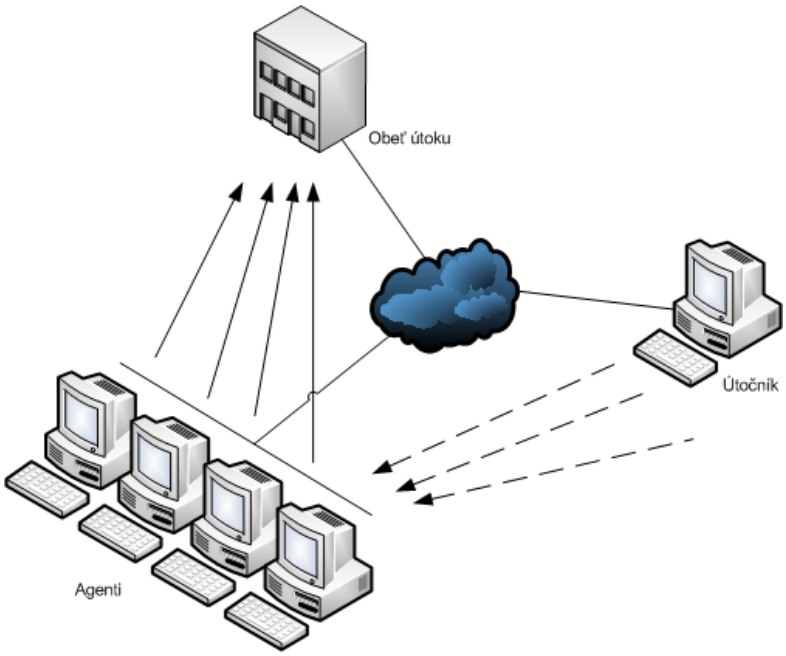
Smurf používa broadcast správu k zaplaveniu cieľového systému. Začína to tak, že útočník pošle veľké množstvo ICMP žiadostí na broadcast adresu siete s potvrdenou falošnou zdrojovou IP adresou. Smerovač uskutoční funkciu broadcast a väčšina staníc odpovie ICMP echo reply. Vo viac prístupovej broadcastovej sieti môže byť niekoľko desiatok až stoviek staníc, ktoré odpovedajú na každý echo paket.



Obr. 2.6: Útok Smurf

2.10.2 **Distributed Denial of Service**

Distribuované DoS [10] útoky koordinovane používajú niekoľko systémov v rôznych miestach k útoku na konkrétnu obeť a je zložité ich dohľadať. Útočníci ohrozia niekoľko systémov v Internete inštaláciou škodlivého kódu, aby mohli zahájiť koordinované útoky. Tieto systémy sa často označujú ako boti. Tieto útoky charakteristicky zhoršujú priepustnosť a ďalšie sieťové zdroje.



Obr. 2.7: Distribuovaný DoS útok.

2.10.3 **Session hijacking**

Session hijacking alebo „únos“ nastane, keď útočník zachytí spojenie alebo reláciu medzi dvomi systémami alebo užívateľmi. Najčastejší typ útoku sa používa na základe TCP spojenia a zdrojovo smerovaných paketov. Útočník je umiestnený medzi dvomi systémami a TCP pakety sú smerované cez jeho systém.

Obr.2.8: Session hijacking

2.10.4 **Sniffing**

Je to metóda odpočúvania počítačovej siete. Pri sniffingu dochádza k ukladaniu paketov, ktoré sa posielajú po sieti. Používa sa pri diagnostike siete, zisťovanie používaných služieb a protokolov a odpočúvaniu dátovej komunikácie. V týchto paketoch, ak nie sú kryptované, je možné zobraziť užívateľské meno a heslo.

2.10.5 **XSS**

Cross-site scripting (XSS) je metóda narušenia www stránok využitím bezpečnostných chýb v skriptoch. Útočník vďaka týmto chybám v zabezpečení aplikácie dokáže do stránok vložiť vlastný skript, čo môže využiť buď k poškodeniu vzhľadu stránky, jej výpadku alebo dokonca k získavaniu citlivých údajov.

2.10.6 **SQL injection**

Je to technika napadnutia databázovej vrstvy programu vsunutím kódu cez neošetrený vstup a vykonanie vlastného SQL príkazu. Toto chovanie vzniká pri prepojení aplikačnej vrstvy s databázovou vrstvou a zabraňuje sa mu pomocou potencionálne nebezpečných znakov. V klasickom prípade je útok na internetové stránky vykonaný cez neošetrený formulár, manipuláciou s URL.

3 Implementácia

3.1 Popis bezpečnostnej brány

Testovanie a implementácia jednotlivých konfiguračných nastavení bola realizovaná na zariadení Cisco ASA 5505 [11]. Tento typ bezpečnostnej brány je určený skôr pre malé firmy alebo pobočky, ktoré vyžadujú cenovo dostupné riešenie pre bezpečný prístup k Internetu.

Obr. 3.1 Cisco ASA 5505

Táto bezpečnostná brána ponúka integrovaný 8 portový fastethernetový switch. Tento switch je možné užívateľsky nakonfigurovať a napríklad jeden port vyhradiť pre pripojenie serveru do demilitarizovanej zóny.

Obsahuje integrovaný IDS systém, ktorý chráni sieť pred známymi útokmi, filtrovanie Java apletov [12] a URL [13], ktorým môžeme kontrolovať, ktoré www stránky sú navštevované.

Umožňuje premávku VPN, buď pre vzdialeným prístupom užívateľov do vnútornej siete použitím klienta alebo trvalým pripojením k pobočke alebo firme.

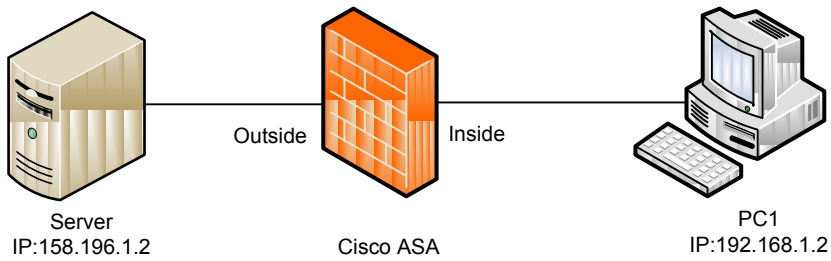
Správa bezpečnostnej brány je pomocou pripojenia cez sériovú linku na konzolu alebo vzdialený prístup pomocou komunikačných kanálov SSH [14], Telnet [15], www prístup pomocou ASDM, pri ktorom vyžaduje internetový prehliadač s podporou Javy.

Počet staníc vo vnútornej sieti a rôzne konfiguračné nastavenia sú obmedzené v závislosti na inštalovanej licencii.

3.2 Pripojenie k bezpečnostnej bráne

Pripojenie k bezpečnostnej bráne sa realizuje pomocou konzolového kábla, s ktorým sa prepojí konzolové rozhranie a sérové rozhranie na počítači. Počítač komunikuje s bezpečnostnou bránou cez terminál, napríklad Minicom [16]. Po nastavení vzdialeného prístupu a http servera, je prístupný webový nástroj ASDM.

3.3 Základná konfigurácia ASA



Obr3.2 Základné schéma

Na obrázku 3.3 je znázornené pripojenie malej siete k Internetu. Počítač PC1 pristupuje k serveru cez bezpečnostnú bránu, ktorá používa PAT k prekladu vnútornej IP adresy na verejnú adresu cez vonkajšie rozhranie. K pripojeniu počítača je potrebné vytvoriť virtuálne rozhranie LAN (VLAN) [17] pre vnútorné rozhrania a priradiť k nej fyzické rozhranie. To isté aj pre vonkajšie rozhranie.

Konfigurácia vnútorného VLAN rozhrania:

```
ciscoasa(config)# interface Vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Konfigurácia vonkajšieho VLAN rozhrania:

```
ciscoasa(config)# interface Vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip address 158.196.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

V uvedenej konfigurácii sa nachádzajú dva parametre, ktoré určujú úrovne zabezpečenia. Medzi každými dvomi rozhraniami nájdeme jedno rozhranie s vyššou a jedno s nižšou úrovňou.

Security-level alebo úroveň zabezpečenia určuje, či dané rozhranie je považované vo vzťahu k inému rozhraniu za vnútorné (dôveryhodné) alebo vonkajšie (nedôveryhodné). Rozhranie sa považuje za vnútorné, pokiaľ je jeho úroveň zabezpečenia číselne vyššia ako úroveň zabezpečenia druhého rozhrania. Ak je úroveň nižšia, považuje sa toto rozhranie za vonkajšie.

Hodnoty úrovne zabezpečenia sa pohybujú v intervale 0 až 100:

- *Úroveň zabezpečenia 100* – je to najvyššia úroveň zabezpečenia. Používa sa pre vnútorné rozhranie (inside), je to implicitná hodnota a nedá sa zmeniť. Je to maximálne dôveryhodné rozhranie a mala by byť za ním celá vnútorná sieť.
- *Úroveň zabezpečenia 0* – je to najnižšia úroveň zabezpečenia. Používa sa pre vonkajšie rozhranie (outside), je to opäť implicitná hodnota nedá sa zmeniť. Je to maximálne nedôveryhodné rozhranie a mala by byť za ním nachádzať celá vonkajšia sieť.
- *Úroveň zabezpečenia 1 až 99* – tieto úrovne zabezpečenia môžu byť priradené k jednotlivým ďalším rozhraniam, napríklad DMZ (demilitarizovaná zóna) [18].

Príkazom *nameif* sa priradí danému rozhraniu názov a úroveň zabezpečenia. Výnimkou sú vnútorné a vonkajšie rozhrania, pretože ich názvy *inside* a *outside* sú nastavené implicitne.

Po vytvorení VLAN rozhraní, je potrebné k nim priradiť jednotlivé fyzické rozhrania. To sa realizuje pomocou príkazu *switchport access vlan <id>*.

Priradenie rozhrania Ethernet 0/0 do VLAN 2:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shutdown
```

Ďalšie dva príkazy zapnú rozhranie Ethetnet 0/1 a použijú sa tiež pre zapnutie ostatných rozhraní, teda Ethernet 0/2 až 0/7 a sú automaticky priradené do VLAN 1.

```
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# no shutdown
```

Aby sa mohli dáta odosielať do vonkajšej siete, je potrebné nastaviť preklad adries a povoliť premávku v prístupovom zozname.

Preklad adries NAT:

```
ciscoasa(config)# nat (inside) 1 192.168.1.0 255.255.255.0
ciscoasa(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

Povolenie odosielanie a prijímanie ICMP paketov:

```
ciscoasa(config)# access-list ping extended permit icmp any any echo
ciscoasa(config)# access-list ping extended permit icmp any any
echo-reply
ciscoasa(config)# access-list ping extended permit ip any any
```

Výpis preložených adries NAT príkazom *sh xlate* :

```
ciscoasa(config)# sh xlate
2 in use, 2 most used
Global 209.165.201.3 Local 192.168.1.2
Global 209.165.201.4 Local 192.168.1.5
```

Otestovanie komunikácie nástrojom hping2:

```
hping2 -1 158.196.1.2
HPING 158.196.1.2 (eth0 158.196.1.2): icmp mode set, 28 headers + 0
data bytes
len=46 ip=158.196.1.2 ttl=64 id=20527 icmp_seq=0 rtt=0.7 ms
len=46 ip=158.196.1.2 ttl=64 id=20528 icmp_seq=1 rtt=0.3 ms
len=46 ip=158.196.1.2 ttl=64 id=20529 icmp_seq=2 rtt=0.3 ms
```

3.4 NAT Control

Riadenie NAT alebo NAT Control [19] vyžaduje, aby sa pakety prechádzajúce z vnútorného rozhrania do vonkajšieho rozhrania zhodovali s NAT pravidlami. Rozhrania s rovnakou úrovňou zabezpečenia nevyžadujú použiť NAT. Ak konfigurujeme dynamický NAT alebo PAT s rovnakou úrovňou na rozhraní, potom sa musí celá premávka porovnávať s NAT pravidlami. Riadenie NAT nemá vplyv na statický NAT a nespôsobuje obmedzenie ako pri použití dynamického NAT.

Ak sa povolí kontrola NAT, potom užívatelia vo vnútornej časti sa musia zhodovať s pravidlami pred vstupom do vonkajšej časti. Ak sa nevyžaduje preklad NAT pre niekoľkých užívateľov, je možné sa prekladu vyhnúť, ak niektorý užívatelia používajú aplikácie, ktoré nepodporujú NAT.

Požiadavky:

- Pakety prechádzajúce z vnútorného rozhrania na vonkajšie sa musia zhodovať s NAT pravidlami.
- Rozhranie s rovnakou úrovňou zabezpečenia nevyžaduje používať pri komunikácii NAT. Ak sa nastaví dynamický NAT alebo PAT s rovnakou bezpečnosťou rozhrania, potom celá premávka z rozhrania s rovnakou úrovňou zabezpečenia sa musí zhodovať s NAT pravidlom.
- Statický NAT s použitím riadenia NAT nespôsobuje tieto obmedzenia.

3.4.1 Identita NAT

Pri konfigurácii identity NAT sa nemusí obmedzovať preklad pre užívateľov na špecifickom rozhraní, ale musí sa použiť pre pripojenie cez všetky rozhrania. Preto sa nemôže vybrať normálny preklad na reálne adresy pre prístup na rozhranie , ale použije sa identita NAT pri výstupe na rozhranie. Aj keď je mapovaná adresa rovnaká ako skutočná adresa, nemôže vytvoriť spojenie z vonkajšej časti do vnútornej, pričom môže byť povolený prístup v prístupovom zozname.

Identita NAT sa povoľuje príkazom *nat 0* a umožňuje adrese užívateľa alebo podsieti preložiť adresu. Bezpečnostná brána neprekladá odchádzajúce spojenia z vnútornej siete 192.168.2.0/24.

```
ciscoasa(config)# nat (inside) 0 192.168.1.0 255.255.255.0
```

3.4.2 Statická identita NAT

Umožňuje určiť rozhranie, na ktorom chceme povoliť používanie reálnych adries pri prístupe na rozhranie a použiť regulárny preklad na výstupnom rozhraní. Statická identita tiež používa NAT politiky, ktoré identifikuje reálne a cieľové adresy pri určovaní prekladu na skutočnú adresu.

```
ciscoasa(config)# access-list inside_nat permit ip host 192.168.1.5
host 158.196.1.4
ciscoasa(config)# static (inside,outside) 209.165.201.20 access-list
inside_nat
```

Definovaná politika prekladu zdrojovej adresy na 209.165.201.20, ak pakety pochádzajú od užívateľa 192.168.1.5 a smerujú na adresu 158.196.1.4.

3.4.3 NAT výnimka

Umožňuje prekladať a zároveň vytvoriť spojenie vzdialeným užívateľom. Nemusí sa obmedzovať preklad pre hostiteľov na špecifické rozhrania, musí sa použiť výnimka pre pripojenie cez všetky rozhrania. NAT výnimka dáva možnosť určiť skutočné a cieľové adresy pri preklade na reálne adresy.

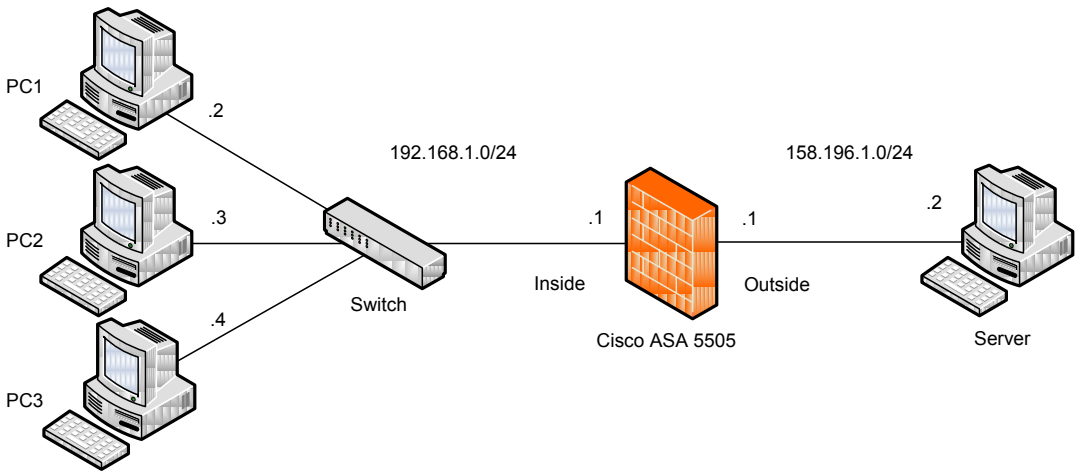
```
ciscoasa(config)# access-list servery extended permit ip host
192.168.1.5 host 192.168.1.7
ciscoasa(config)# nat (inside) 0 access-list servery
ciscoasa(config)# nat (inside) 1 192.168.1.0 255.255.255.0
ciscoasa(config)# global (outside) 1 interface
```

Prístupový zoznam pomenovaný *servery* identifikuje dva emailové servery a tie sú spojené príkazom *nat 0* ohraničené vnútorným rozhraním. Ostatná premávka z vnútornej siete 192.168.1.0/24 je prekladaná na adresu vonkajšieho rozhrania.

3.5 Povoľovanie služieb

V základnom nastavení bezpečnostnej brány sú všetky služby zakázané. Preto je nutné každú potrebnú službu povoliť jednotlivo. Je to nastavené z bezpečnostného hľadiska, aby sa nemuselo zisťovať, ktoré služby sú povolené navyše a tým sa neohrozovala bezpečnosť vnútornej siete.

V schéme zapojenia, zobrazenej na obrázku 3.4, sú povolené služby pre prístup k webovým serverom, používanie prenosu dát cez FTP [20], služby pre príjem a odosielanie elektronickej pošty a vzdialený prístup k jednotlivým aktívnym prvkom vo vnútornej sieti pomocou Telnetu a SSH. Pravidlá sú aplikované na vnútorné rozhranie. To znamená, že kontrola nastáva vždy pri vchádzaní a vychádzaní paketov cez dané rozhranie.



Obr. 3.4 Schéma zapojenia pri povoľovaní služieb

Povolenie služieb HTTP a HTTPS:

```
ciscoasa(config)#access-list 100 extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq www
ciscoasa(config)#access-list 100 extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq https
ciscoasa(config)# access-list 100 extended permit ip any any
ciscoasa(config)# access-group 100 in interface inside
```

Služba FTP :

```
ciscoasa(config)# access-list ftp extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq ftp-data
ciscoasa(config)# access-list ftp extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq ftp
ciscoasa(config)# access-group ftp in interface inside
```

Odchytávanie premávky služieb elektronickej pošty:

```
ciscoasa(config)# access-list mail extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq smtp
ciscoasa(config)# access-list mail extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq pop3
ciscoasa(config)# access-list mail extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq imap4
ciscoasa(config)# access-list mail extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq 465
ciscoasa(config)# access-list mail extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq 995
ciscoasa(config)# access-group mail in interface inside
```

Vzdialený prístup SSH a Telnet:

```
ciscoasa(config)# access-list remote extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq ssh
ciscoasa(config)# access-list remote extended permit tcp 192.168.1.0
255.255.255.0 host 158.196.1.2 eq telnet
ciscoasa(config)# access-group remote in interface inside
```

3.6 Skupina objektov

Vytvorením skupín objektov [21] sa zredukuje počet prístupových pravidiel. Konfigurácia bezpečnostnej brány môže obsahovať až tisíc riadkov pravidiel a správa zariadenia je zložitá. S použitím skupín objektov sa zmenší počet použitých pravidiel vytvorením jednotlivých zoznamov. Pomocou týchto objektov môžeme zoskupovať sieťové objekty, napríklad vnútorné servery do jednej skupiny a užívateľov do ďalšej skupiny. Bezpečnostná brána môže tiež kombinovať TCP [22] služby do jednej a vytvoriť skupinu týchto služieb.

Typy objektov:

- Protokol
- Sieť
- Služba

Skupina objektov typu Protokol kombinuje IP protokoly, ako sú TCP, UDP [23] a ICMP [24], do jedného objektu.

```
ciscoasa(config)# object-group protocol TCP
ciscoasa(config-protocol)# protocol-object tcp
```

Sieťové objekty špecifikujú zoznam IP adries užívateľov, podsiete alebo celej siete.

```
ciscoasa(config-protocol)# object-group network Vnutorne_PC
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# network-object host 192.168.1.5
```

Objekty typu služba sa používajú k zoskupeniu TCP alebo UDP služieb a môžeme vytvoriť skupinu TCP, UDP, alebo TCP a UDP portov do jedného objektu. Ďalej umožňuje vytvoriť skupinu, ktorá obsahuje jednotlivé TCP služby, UDP služby a rôzne ďalšie služby.

```
ciscoasa(config-network)# object-group service HTTP-SSH
ciscoasa(config-service)# service-object tcp http
ciscoasa(config-service)# service-object tcp ssh
```

Po vytvorení jednotlivých objektov sa aplikujú pomocou prístupových pravidiel ACL a to sa priradí na rozhranie.

3.7 Adaptive Security Device Manager

ASDM [25] je intuitívny nástroj s webovým rozhraním, ktorý slúži pre konfiguráciu, správu a monitorovanie bezpečnostnej brány. Toto webové rozhranie je prístupné z ľubovoľnej časti v sieti a poskytuje administratívne nástroje a monitorovacie funkcie.

Spustenie a inštalácia nástoja ASDM vyžaduje konfiguráciu HTTP [26] servera a vzdialený prístup SSH na bezpečnostnej bráne. Ďalšou podmienkou inštalácie webového rozhrania je použitie internetového prehliadača s podporou Javy [27].

Inštalácia HTTP servera:

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

Nastavenie cesty pre obrazu ASDM:

```
ciscoasa(config)# asdm image flash: asdm-621.bin
```

Konfigurácia SSH:

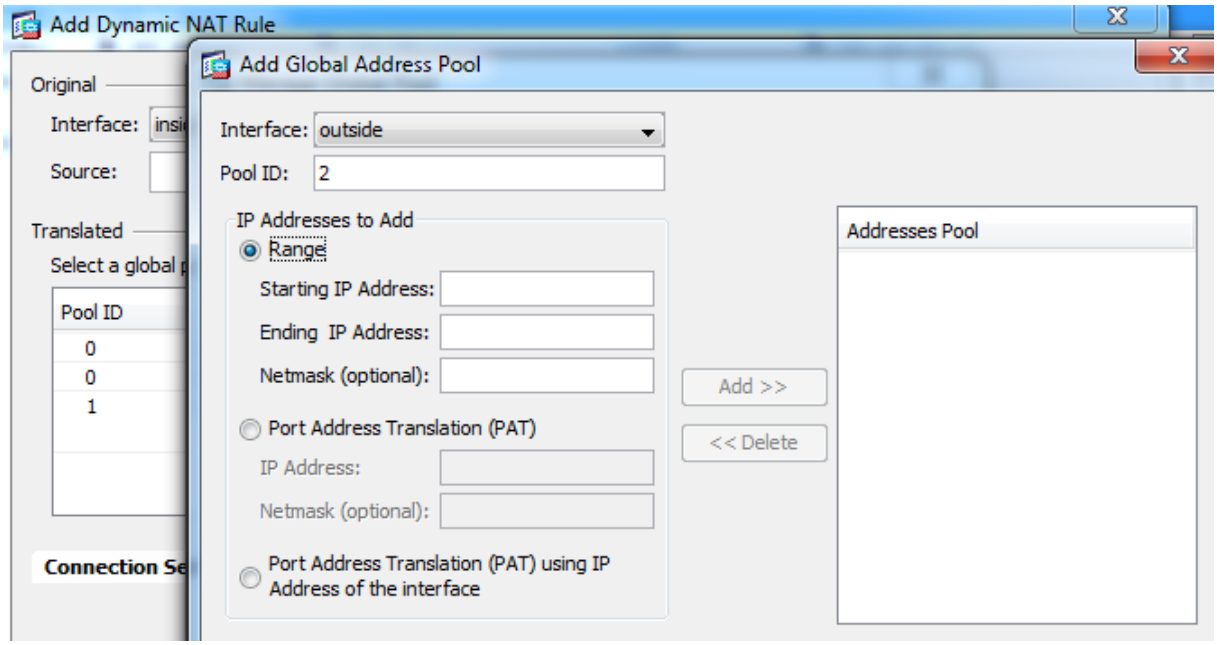
```
ciscoasa(config)# enable password cisco
ciscoasa(config)# username cisco password cisco
ciscoasa(config)# ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)# domain-name cisco.org
ciscoasa(config)# crypto key generate rsa modulus 1024
```

Po nastavení týchto častí zadáme do prehliadača adresu *https://192.168.1.2/admin* a zobrazí sa úvodná stránka s možnosťou inštalácie do počítača. Po stiahnutí obrazu ASDM a následnej inštalácii, sa dostaneme do webového rozhrania bezpečnostnej brány, kde sú zobrazené rôzne monitorovacie funkcie a konfiguračné možnosti.

Na obrázku 3.5 je zobrazený formulár pre vytvorenie pravidla ACL. Nachádzajú sa v ňom možnosti výberu akcie, výber zdrojovej časti, napríklad konkrétny počítač, podsieť alebo celá sieť, cieľovej časti, napríklad konkrétna stanica alebo celá vonkajšia sieť, a služba ktorú chceme povoliť alebo zakázať.

Obr. 3.5 Vytvorenie pravidla ACL

Obrázok 3.6 zobrazuje formulár konfigurácie dynamického NAT, v ktorom sa určuje, na ktoré rozhranie bude umiestnený. Ďalej je možnosť výberu adresného rozsahu, nastavenie prekladu PAT s pridelenou adresou alebo PAT s adresou umiestnenom na rozhraní.



Obr. 3.6 Konfigurácia dynamického NAT

3.8 Overenie konfigurácie

Vytvorená konfigurácia a jej komunikácia cez bezpečnostnú bránu bola testovaná pomocou sieťových nástrojov hping2, Wireshark a Packet Tracer v prostredí ASDM. Na vonkajšom počítači s IP adresou 158.196.1.2 boli simulované otvorené komunikačné porty v operačnom systéme Linux Ubuntu pomocou príkazu:

```
nc –l <číslo portu>
```

3.8.1 Hping2

Hping [27] je sieťový nástroj, ktorý generuje a analyzuje pakety protokol ICMP, TCP a UDP. Tento nástroj slúži k overovaniu bezpečnosti, testovaniu firewallov a sietí. Vytvorí ľubovoľné telo a veľkosť paketu a je možné ho poslať pod podporovanými protokolmi.

Analýza TCP paketov:

- *TCP SYN/ACK* – paket je prijatý na firewall a odoslaný na cieľovú stanicu, port je otvorený.
- *TCP RST/ACK* – paket je prijatý na firewall, ale je zastavený pravidlom v jeho politike.
- *ICMP type 3 code 13* – ak je prijatý paket v tomto tvare, užívateľ má obmedzené spojenie v zozname ACL.
- *Žiadna odpoveď* – ak nie je prijatý paket, bezpečnostné zariadenie ho zahodí.

Otvorený TCP port 80 (HTTP):

```
hping2 -S -c 3 -p 80 158.196.1.2
HPING 158.196.1.2 (eth0 158.196.1.2): S set, 40 headers + 0 data
bytes
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=80 flags=SA seq=0
win=5840 rtt=0.6 ms
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=80 flags=SA seq=1
win=5840 rtt=0.6 ms
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=80 flags=SA seq=2
win=5840 rtt=0.6 ms
```

Otvorený TCP port 25 (SMTP):

```
hping2 -S -c 3 -p 25 158.196.1.2
HPING 158.196.1.2 (eth0 158.196.1.2): S set, 40 headers + 0 data
bytes
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=25 flags=SA seq=0
win=5840 rtt=0.6 ms
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=25 flags=SA seq=1
win=5840 rtt=5.2 ms
len=48 ip=158.196.1.2 ttl=64 DF id=0 sport=25 flags=SA seq=2
win=5840 rtt=5.1 ms
```

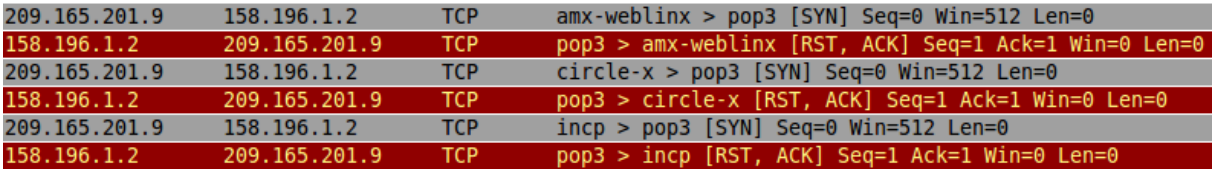
Zatvorený TCP port 443 (HTTPS):

```
hping2 -c 3 -p 443 158.196.1.2
HPING 158.196.1.2 (eth0 158.196.1.2): NO FLAGS are set, 40 headers +
0 data bytes
len=46 ip=158.196.1.2 ttl=255 id=49266 sport=443 flags=RA seq=0
win=512 rtt=0.4 ms
len=46 ip=158.196.1.2 ttl=255 id=46047 sport=443 flags=RA seq=1
win=512 rtt=0.3 ms
len=46 ip=158.196.1.2 ttl=255 id=47347 sport=443 flags=RA seq=2
win=512 rtt=0.3 ms
```

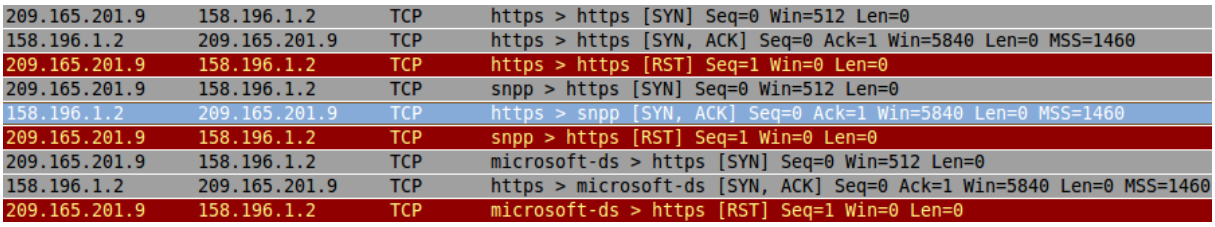
TCP SYN (synchronizačné) pakety sú odoslané na cieľové porty 25, 80 a 443 s cieľovou adresou 158.196.1.2. V prvom a druhom prípade obsahuje správa parameter SA, teda *Synchronizated* a *Acknowledge,* kde klient pošle na server paket s príznakom SYN, server uzná jeho ACK a odošle paket s príznakmi SYN/ACK. To znamená, že port je otvorený a môže na ňom prebiehať komunikácia. V treťom prípade obsahuje správa parameter RA, teda *Restrict* a *Acknowledge,* a služba na tomto porte je obmedzená bezpečnostnou bránou a prichádzajúce pakety sú zahodené firewallom.

3.8.2 Wireshark

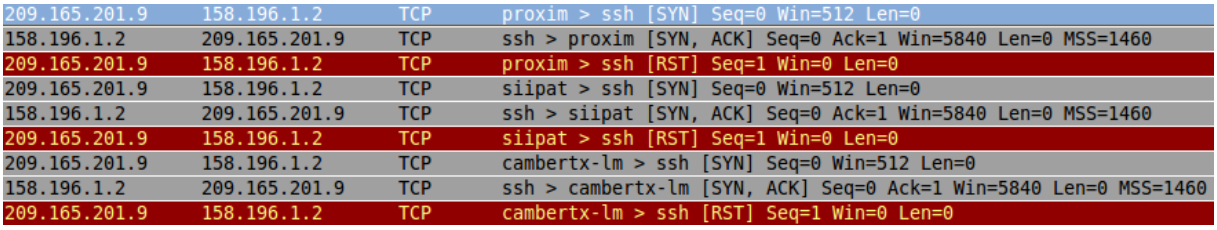
Je to protokolový analyzátor a medzi jeho najčastejšie použitie patrí analýza a problémy sieťovej komunikácie v počítačových sieťach. Aplikácia obsahuje rôzne analyzátory komunikačných protokolov, grafické užívateľské rozhranie a možnosti filtrovania zobrazených informácii. Sieťovú kartu vie prepnúť do tzv. promiskuitného režimu a teda môže zachytávať celú komunikáciu na médiu.



Obr. 3.7 Výpis zachytenia služby POP3



Obr. 3.8 Výpis zachytenia služby HTTPS



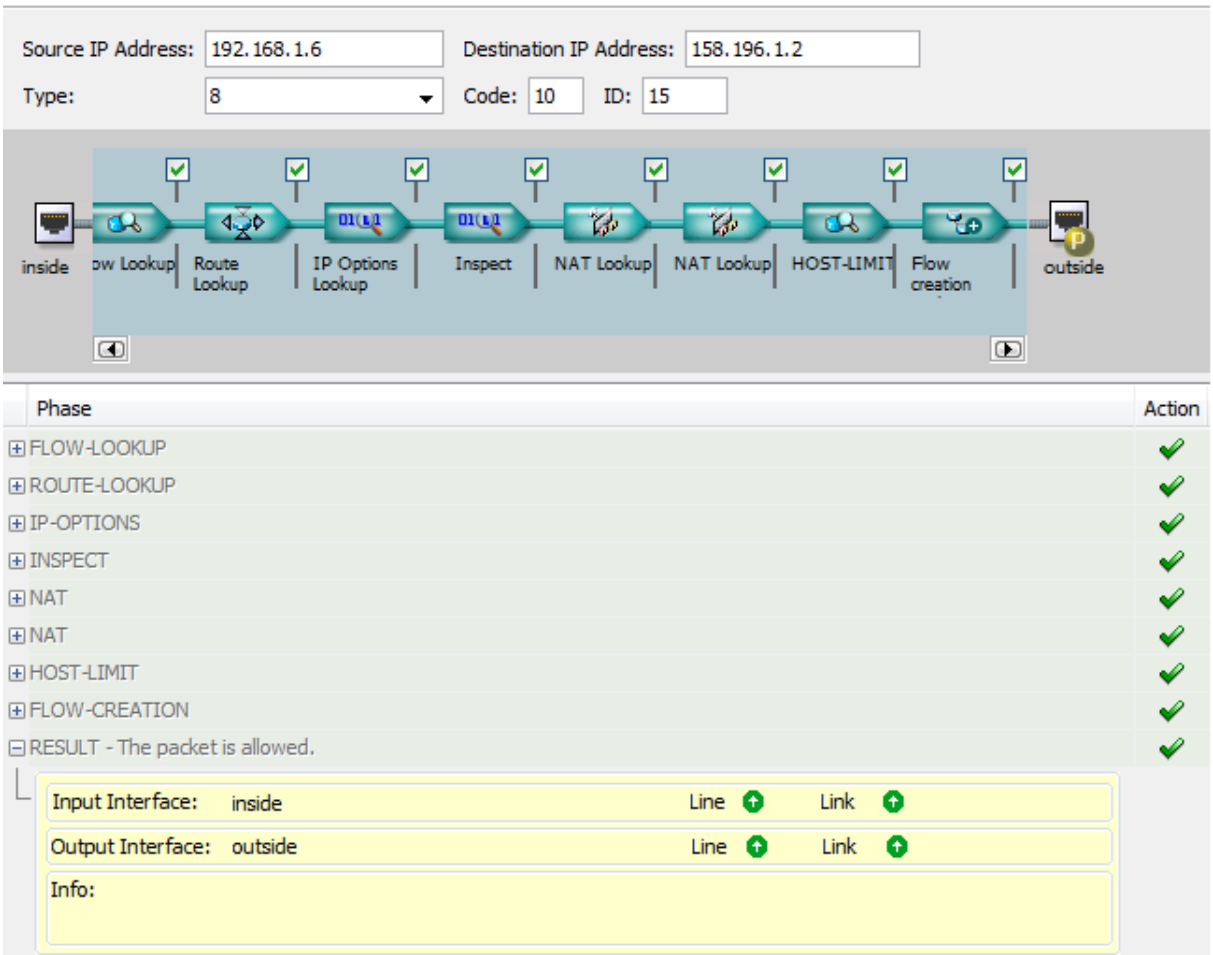
Obr. 3.9 Výpis zachytenia služby vzdialeného prístupu SSH

Na obrázkoch 3.7, 3.8 a 3.9 sú zobrazené zachytené pakety služieb pre príjem elektronickej pošty POP3 [28], šifrovaný prenos pomocou HTTPS [29] a vzdialený prístup SSH. Táto komunikácia bola zachytená na simulovanom serveri vo vonkajšej sieti. Zdrojová adresa 209.165.201.9 je preložená vnútorná adresa 192.168.1.2 pomocou NAT.

3.8.3 Packet Tracer

Tento sieťový nástroj uľahčuje trasovať aplikovanie zložitých bezpečnostných pravidiel v prostredí ASDM. Animácia toku dát uľahčí orientáciu, správca emuluje dátové toky na vybrané sieťové zdroje a skúša platnosť nastavených pravidiel. Tento spôsob grafického znázornenia urýchľuje vývoj bezpečnostných politík a pomôže odladiť chyby v nastavení.

Na obrázku 3.11 je znázornené overenie služby ICMP z vnútornej siete a IP adresou 192.168.1.6, do vonkajšej siete s IP adresou 158.196.1.2. Z obrázku vyplýva, že konfigurácia služby ICMP na bezpečnostnej bráne je správna.



Obr. 3.11 Overenie služby ICMP v nástroji Packet Tracer

4 Záver

Téma bezpečnosť počítačovej siete je na popredných miestach riešených problémov. Okrem samotnej ochrany dát a odopretiu prístupu neautorizovaným osobám, bezpečnosť obsahuje aj detekciu nežiaducej udalosti, prevenciu, ktorá sa vykonáva podľa daných krokov pri detekcii útoku.

Jeden z hlavných dôvodov vzniku tejto bakalárskej práce bolo zoznámiť sa s problematikou práce s bezpečnostnou bránou a filtračnými technikami. Vytvoriť návrh riešenia a následne implementovať konfigurácie na fyzické zariadenie a tieto riešenia overiť v laboratóriu pomocou sieťových nástrojov.

Po oboznámení sa práce s bezpečnostnou bránou, bol vytvorený návrh riešenia pripojenia vnútornej siete do vonkajšej siete. K prepojeniu týchto dvoch sietí bol použitý dynamický preklad adries NAT a k nemu pridelený rozsah adries. K prístupu vnútornej siete do vonkajšej bolo potrebné vytvoriť rôzne prístupové pravidlá pre niektoré služby, ktoré sú určené pre komunikáciu s vonkajším svetom, pretože v základnom nastavení sú všetky služby zakázané. Tieto vytvorené pravidlá boli rozdelené do rôznych skupín objektov, ktoré pomohli zjednodušiť a sprehľadniť celú konfiguráciu. Pri správe bezpečnostnej brány bolo pomerne často používané webové rozhranie ASDM, ktoré vynikalo svojou jednoduchosťou a intuitívnymi možnosťami.

Počas práce bolo na zariadení otestovaných niekoľko konfiguračných nastavení, ktoré boli po implementácii otestované niekoľkými sieťovými nástrojmi, ktoré tiež pomáhali odhaľovať jednotlivé problémy a nedostatky pri nesprávne zadanej konfigurácii a parametroch. Najpoužívanejšou testovacou službou spojenia medzi počítačmi cez bezpečnostnú bránu bola služba PING, ktorá odhaľovala časté problémy komunikácie. Problémy s komunikáciou a konfiguráciou pomáhalo odhaľovať aj webové rozhranie ASDM so zapnutou funkciou logovania.

Prínosom tejto práce sú určite skúsenosti s konfiguráciou a so správou bezpečnostnej brány, s tvorbou bezpečnostných nastavení a s testovaním.

Do budúcnosti by bolo určite zaujímavé vytvoriť ďalšie návrhy zapojení a otestovať rôzne ďalšie možnosti bezpečnostnej brány, pretože táto téma je pomerne rozsiahla na nejednu bakalársku alebo diplomovú prácu.

Použitá literatúra

[1] Velký průvodce protokoly TCP/IP a systémem DNS. 5. vyd. Brno: Computer Press, 2008. ISBN 987-80-251-2236-5.

[2] CCNA: Výukový průvodce přípravou na zkoušku 640-802. 1. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2359-1.

[3] Configuration NAT. *Cisco* [online]. 2010 [cit. 2012-03-28]. Dostupné z: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cfgnat.html#wp1043190

[4] NAT. *Network Address Translation - NAT* [online]. 2010 [cit. 2012-03-29]. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/NAT/Nat.htm

[5] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance:PAT*. 2. vyd. Indianapolis: cisco press, 2009, s. 212-215. ISBN 9781587058196.

[6] Samuraj-cz. *IPsec VPN a Cisco* [online]. 2011 [cit. 2012-04-02]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

[7] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*: *IDS*. 2. vyd. Indianapolis: ciscopress, 2009, s. 8-9. ISBN 9781587058196.

[8] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*: *IPS*. 2. vyd. Indianapolis: ciscopress, 2009, s. 10-12. ISBN 9781587058196.

[9] Lupa.cz. *Denial of Service (DoS) útoky* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-dos-utoky-uvod/

[10] Diit.cz. *DDoS utok* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[11] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*: *Cisco ASA 5505*. 2. vyd. Indianapolis: ciscopress, 2009, s. 26-29. ISBN 9781587058196.

[12] Wikipedia. *Java applet* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://en.wikipedia.org/wiki/Java_applet

[13] Wikipedia. *Uniform Resource Locator* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Uniform_Resource_Locatorlet

[14] Wikipedia. *Secure Shell* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Secure_Shellesource_Locatorlet

[15] Wikipedia. *Telnet* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Telnet

[16] Minicom. *Minicom* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://alioth.debian.org/projects/minicom

[17] *Interconnecting Cisco Network Devices, Part 2 (ICND2)*: *VLAN*. 3. vyd. Indianapolis: cisco press, 2008, s. 13-63. ISBN 9871587054631.

[18] *Velký průvodce protokoly TCP/IP a systémem DNS*: *DMZ*. 5. vyd. Brno: Computer Press, 2008, s. 466-467. ISBN 987-80-251-2236-5.

[19] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*: *NAT Control*. 2. vyd. Indianapolis: Cisco Press, 2009, s. 216-224. ISBN 9781587058196.

[20] Wikipedia. *File Transfer Protocol* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/File_Transfer_Protocol

[21] *Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*: *Object group*. 2. vyd. Indianapolis: Cisco Press, 2009, s. 159-166. ISBN 9781587058196.

[22] Wikipedia. *Transmission Control Protocol* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Transmission_Control_Protocol

[23] Wikipedia. *User Datagram Protocol* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/User_Datagram_Protocol

[24] Wikipedia. *ICMP* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/ICMP

[25] Cisco.com. *Cisco Adaptive Security Device Manager* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://www.cisco.com/en/US/products/ps6121/index.html

[26] Wikipedia. *Hypertext Transfer Protocol* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[27] THE SPRAWL. *Research hping* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://www.thesprawl.org/research/hping/

[28] Wikipedia. *Post Office Protocol* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/Post_Office_Protocol_version_3

[29] Wikipedia. *HTTPS* [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://cs.wikipedia.org/wiki/HTTPS

Obsah priloženého CD

Obsah jednotlivých priečinkov priloženého CD:

- *Bakalarska_praca* – obsahuje text tejto práce vo formáte pdf
- *Konfiguracia* – obsahuje výpis konfigurácie z bezpečnostnej brány